الجرائم الإلكترونية المفهوم والأسباب

Diab Al-Badayneh
Ibn Khaldun Center for Research and Studies (IKCRS), Jordan

كلية العلوم الإستراتيجية

الملتقى العلمي

الجرام المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية

خلال الفترة من: ٧ ـ ٩/١١/١٤٣٥هـ الموافق ٢ ـ ٤/٩/٢٠١٤م

ورقة علمية بعنوان

الجرائم الإلكترونية: المفهوم والأسباب

إعـداد

أ.د. ذيــاب موســى البداينــة

عمان – المملكة الأردنية الهاشمية

١٤٣٥هـ - ٢٠١٤م

الجرائم الإلكترونية: المفهوم والأسباب

الأستاذ الدكتور ذياب البداينة
كلية الشرطة
وزارة الداخلية
قطر
٩٧٤٥٥٥٠٦٦٤٢

ورقة مقدمة في الملتقى العلمي الجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية والدولية ٢-٢٠١٤/٩/٤
عمان -الاردن

الجرائم الإلكترونية: المفهوم والأسباب

الأستاذ الدكتور ذياب البداينة
كلية الشرطة
وزارة الداخلية
قطر
٩٧٤٥٥٥٠٦٦٤٢

الملخص

تتكون الجريمة الإلكترونية أو الافتراضية (cyber crimes) من مقطعين هما الجريمة (crime) والإلكترونية (cyber). ويستخدم مصطلح الإلكترونية لوصف فكرة جزء من الحاسب أو عصر المعلومات. أما الجريمة فهي السلوكيات والأفعال الخارجة على القانون. والجرائم الإلكترونية هي " المخالفات التي ترتكب ضد الأفراد أو المجموعات من الأفراد بدافع الجريمة وبقصد إيذاء سمعة الضحية أو أذى مادي او عقلي للضحية مباشر او غير مباشر باستخدام شبكات الاتصالات مثل الإنترنت (مثل غرف الدردشة، والبريد الإلكتروني، والموبايل) (Halder & Taishankar, 2011). ويمثل جوهر الجريمة الإلكترونية. أبعد من هذا الوصف، ومع ذلك، فالأعمال ذات الصلة بالحاسوب لأغراض شخصية أو تحقيق مكاسب مالية أو ضرر، بما في ذلك أشكال الجرائم المتصلة بالهوية، والأفعال المتعلقة بمحتويات الكمبيوتر جميعها تقع ضمن معنى أوسع لمصطلح "الجريمة الإلكترونية". (UNODC, 2013).

كما تتناول أسباب الجريمة الإلكترونية، حيث تم تصنيف هذه الأسباب على ثلاثة مستويات من النظم هي: النظام الشخصي، والنظام الوسيط والنظام الكلي. فقد انطلقت من أن الجرائم الإلكترونية هي الأفعال الإجرامية التي ترتكب بواسطة الحاسب أو النطاق التقني مثل الإنترنت والشبكات، أو التي يكون فيها الحاسب والحيز التقني مستهدف للجريمة الإلكترونية. وتشمل الجرائم الإلكترونية ضمن هذا التحديد وليس حصرا على (الإرهاب الإلكتروني، والاحتيال وسرقة الهوية، والملاحقة والتحرش، وبريد النفايات، والفيروسات، وشم كلمات السر، والقنابل الذكية).

وتتلخص أسباب الجرائم الإلكترونية بانها ظاهرة اجتماعية متوافقة مع انتقال المجتمعات إلى المجتمع الرقمي، حيث انتقل نشاط الناس من الواقع الفعلي (المادي) إلى الواقع الافتراضي، وهي جريمة عابرة للحدود الوطنية. وقد سهل انتشار **الجرائم الإلكترونية** سهولة الوصول للمستهدفين وانخفاض الكلفة، والغفلة في تنفيذها وضعف الرقابة والسرعة في تنفيذها وتوظيف الاتصالات والتفاعلات في ارتكابها، وقلة الخطورة على الجناة، وسرعة الكسب غير المشروع، والفرص المتاحة لارتكابها، والضغوط الشخصية والعامة على الجناة، وضعف الرقابة

عامة. كما ساهمت عوامل التحضر السريع، والبطالة والرغبة بسرعة الثراء، وضعف التشريعات وضعف أدوات الحماية، وتوافر الفرصة لارتكابها وغياب الحراسة التقنية في انتشارها. وينفذها شباب يسعون للشهرة أو مجرمون محترفون يسعون للكسب والثراء، أو إرهابيون.

المقدمة

في عام ٢٠١١، كان هناك ٢.٣ مليار شخص على الأقل كان لهم وصول إلى شبكة الإنترنت ، أي ما يعادل أكثر من ثلث إجمالي سكان العالم. وأن أكثر من ٦٠ في المائة من جميع مستخدمي الإنترنت هم من البلدان النامية ، وهناك ٤٥ % من جميع مستخدمي الإنترنت دون سن ٢٥ عاما. كما تشير التقديرات أنه قبل عام ٢٠١٧، فأن اشتراكات (broadband) المتنقل سوف تقترب من ٧٠% من إجمالي عدد سكان العالم. وبحلول العام ٢٠٢٠، فأن عدد أجهزة الشبكة ("إنترنت الأشياء") سيفوق عدد الناس بمعدل (١:٦) ستة إلى واحد، محولين المفاهيم الحالية للإنترنت. في عالم الغد عالم الشبك فائق السرعة ، سيصبح من الصعب أن نتخيل 'الجريمة الإلكترونية "، وربما أي جريمة، لا تنطوي على أدلة الإلكترونية مرتبطة مع بروتوكول الإنترنت (الاتصال (IP) (UNODC, 2013).

تميز القرن ٢١ باستخدام المعلومات، وعلى مدى السنوات القليلة الماضية توسعت الإنترنت أضعافا مضاعفة. حاليا ، حوالي هناك ٨٢٠ مليون شخص يستخدمون الإنترنت ، بزيادة قدرها ١٢٦ في المئة من ٢٠٠٠-٢٠٠٥ (InternetWorldStats.com, 2005). لقد وفرت السهولة النسبية لاستخدام الإنترنت، والحصول على الإنترنت على نحو متزايد أكثر للأنترنت بأسعار معقولة والحصول على أجهزة الكمبيوتر مع أجهزة المودم فائقة السرعة، كل ذلك مكن الناس من التواصل وتكوين الصداقات الجديدة، والتجارة ، والترفيه ، والتعلم، والقيام بأعمال تجارية، ودفع الفواتير عبر الإنترنت. وخلقت شبكة ويب العالمية ما يسمى العالم الافتراضي أو الفضاء الإلكتروني ، والذي يعرف بأنه "مكان لأجل غير مسمى حيث يتفاعل الأفراد والتجمعات " (Britz, 2004, P 2) . ويتصف الفضاء الإلكتروني بأنه مكان بلا حدود مادية أو اجتماعية تحرم الأفراد من العيش فيه.

لقد انتقل الناس من العالم الواقعي إلى العالم الافتراضي، وكذلك انتقلت الجريمة. ولنا إن نتصور حجم التفاعلات التي تتم في الواقع الافتراضي سواء كانت شخصية أو مؤسسية أو في مجال الأعمال أو الخدمات أو الثقافة... فعلى سبيل المثال على الفيس بوك (Facebook) أعجب بصورة أوباما وهو يحتضن زوجة فيما سمي لحظة الفوز ٤ مليون شخص، ومتوسط عدد الأصدقاء على حساب الفيس بوك ١٣٠ صديق وعدد المشتركين ٨٥٠ مليون منهم ٢١% في أسيا، و٤٨٨ مليون يستخدمون الفيس بوك الجوال، و٢٣% من المشتركين يتفقدون حسابهم ٥ مرات في اليوم. وهناك أكثر ن مليون موقع متصل مع الفيس بوك وتوضع ٢٥٠ مليون صورة يومياً، وفي عام ٢٠١٢ تم تشغيل ٢١٠٠٠٠سنة من الموسيقى. من المشتركين ٤٣% ذكور و ٥٧% إناث (Vitality, 2012).

وللأسف، فان الفضاء الإلكتروني ينتج أنواع جديدة من الجريمة تسمى الجريمة الإلكترونية (cyber crimes) من خلال خلق فرص جديدة للمجرمين (Wall, 2005). قد مكنت مجرمي الفضاء الإلكتروني من تصفح الأنترنت وارتكاب جرائم مثل القرصنة، والاحتيال، والتخريب للكمبيوتر ، والإتجار بالمخدرات ، والتعامل في معلومات العدالة، والمواد الإباحية، والملاحقة (United Nations Crime and Justice information UNCJIN, 1999) دون القبض عليهم أو الكشف عن الجرائم. لقد تكونت أنماط جديدة من الجرائم من منها: لصوص الحاسب الذين يدخلون إلى أنظمة الحاسب وقواعد المعلومات ويسرقونها، أو يعبثون بها، والجرائم التي تخترق الحماية الأمنية في النظم القانونية ويتم تجنب العقاب فيها (البداينة، ١٩٩٩).

ووفقا لمكتب إحصاءات العدل فأن (BJS) انخفض معدل جرائم العنف في البلاد ١٠ في المئة في عام ٢٠٠١ واستمر في الانخفاض منذ عام ١٩٩٤. كما سجلت جرائم الإيذاء العنيف والممتلكات أدنى مستوى لها معدلات الجريمة منذ استخدام المسح الوطني لضحايا الجريمة(cvs) في العام 1973 من ناحية أخرى، فإن عدد ضحايا الجريمة الإلكترونية على ارتفاع، نظرا لزيادة في عدد مستخدمي الإنترنت. لقد تزايد عدد ضحايا الجرائم الإلكترونية وخاصة الذين يعانون من خسارة مالية، أو المهددين أو المطاردين، فهي مشكلة تستحق الدراسة. ويمكن دراسة الجريمة الإلكترونية يمكن من خلال وجهات نظر مختلفة، بما في ذلك نظر المجرم أو وجهة نظر الضحية. وتمثل الجريمة الإلكترونية المجال الجديد من الأبحاث في مجال علم الجريمة (Torosyan, 2003).

فقد خلق الفضاء الإلكتروني فرصا جديدة للمجرمين لارتكاب الجرائم من خلال خصائص فريدة من نوعها في هذا الفضاء. ويرى وول (Wall, 2005) أن هذه الميزات تشكل " ;مفاتيح تحويلية " (transformative keys) وهي: (١) **العولمة** (globalization) والتي تمكن الجناة مع وجود فرص جديدة من تجاوز الحدود التقليدية ؛ (٢) "**شبكات التوزيع** (distributed networks)" فقد ولدت فرصاً جديدة لتكوين ضحايا، و(٣) **الإجمالية والشمولية** (synopticism and panopticism)؛ والتي تمكن الجناة منى " اذلال ضحاياهم عن بعد ؛ و(٤) " **مسارات البيانات** " (data trails) والتي خلقت فرصاً جديدة للجنائي لارتكاب سرقة الهوية.

إن المعلومات والبيانات مثلها مثل أية سلعة ذات قيمة مادية عالية عرضة للجريمة بما في ذلك الاحتيال والسرقة والتعدي والتخريب..ألخ. وتزداد جرائم المعلومات يومياً، وأصبحت محط حديث وسائل

الإعلام والباحثين والعلماء. عندما سئل **ويلي سوتن** (Sutton) لماذا سطى على البنك أجاب "لأن المال موجود هناك"، والمال اليوم هو المعلومات، ولقد تعلم المجرمون اليوم مكان وجود المال ويمكنهم سرقة كميات بمخاطرة أقل. ولقد تأزمت العلاقات بين الدول بسبب سرقة المعلومات (أسرار عسكرية تتعلق بتقنيات متقدمة) (والأمثلة على ذلك بين الولايات المتحدة والصين، وكندا، والصين).

لقد أصبحت الجريمة الإلكترونية وجرائم الحاسوب ونظمها، بلا حدود، وهي عالمية، التحقيق فيها والحكم عليها عملية معقدة. وترتكب هذه الجرائم من قبل الأفراد أكثر مما ترتكب من قبل الأفراد أكثر مما ترتكب من قبل محترفي الحاسب وشبكات المعلومات. كما يمكن أن ترتكب من مراكز البحوث، ومن الأكاديميين، ومن مديرين يبحثون عن الثراء أو السلطة، أو من قبل مؤسسات تبحث عن معلومات عن منافسيها، أو من وسائل إعلام تبحث عن معلومات أو أخبار أو من قبل حكومات تبحث عن معلومات تجارية، أو جريمة منظمة تبحث عن ملفات موثوقة (البداينة، ١٩٩٨).

ما هي الجريمة الإلكترونية؟

لا يوجد إجماع على تعريف الجريمة الإلكترونية من حيث كيف تُعرف أو ما هي الجرائم التي تتضمنها الجريمة الإلكترونية. وكما يقول فان دير هلست و ونيف " هناك غياب لتعريف عام واطار نظري متسق في هذا الحقل من الجريمة... وفي أغلب الأحيان تستخدم مصطلحات الافتراضية والحاسوب والإلكترونية والرقمية وكلها تعكس فجوات مهمة في التعريف" (Van der Hulst & Neve, 2008, p.18). ويتراوح تعريف الجريمة الإلكترونية بين الجرائم التي ترتكب بواسطة الحاسوب إلى الجرائم التي ترتكب بأي نوع من المعدات الرقمية (PAC, 2008,P.1). وتعريف الجرائم الإلكترونية باختصار على أنها الجرائم التي ترتكب باستخدام الحاسوب والشبكات والمعدات التقنية مثل الجوال.

تتكون الجريمة الإلكترونية أو الافتراضية (cyber crimes) من مقطعين هما الجريمة (crime) والإلكترونية (cyber). ويستخدم مصطلح الإلكترونية لوصف فكرة جزء من الحاسب أو عصر المعلومات. أما الجريمة فهي السلوكيات والأفعال الخارجة على القانون. والجرائم الإلكترونية هي " المخالفات التي ترتكب ضد الأفراد أو المجموعات من الأفراد بدافع الجريمة وبقصد إيذاء سمعة الضحية أو أذى مادي او عقلي للضحية مباشر او غير مباشر باستخدام شبكات الاتصالات مثل الإنترنت (مثل غرف الدردشة، والبريد الإلكتروني، والموبايل) (Halder & Taishankar, 2011).

وتعتمد تعاريف الجريمة الإلكتروني في الغالب على الغرض من استخدام هذا المصطلح. وتشمل عدداً محدداً من الأعمال ضد السرية والنزاهة وتوافر بيانات الكمبيوتر أو أنظمة . ويمثل جوهر الجريمة الإلكترونية. أبعد من هذا الوصف، ومع ذلك، فالأعمال ذات الصلة بالحاسوب لأغراض شخصية أو تحقيق

مكاسب مالية أو ضرر، بما في ذلك أشكال الجرائم المتصلة بالهوية، والأفعال المتعلقة بمحتويات الكمبيوتر جميعها تقع ضمن معنى أوسع لمصطلح "الجريمة الإلكترونية". (UNODC, 2013).

ولقد خلص فان دير هولست ونفيه (Van der Hulst and Neve, 2008, p. 19) إلى أن: "حقل علم الجريمة يفتقر إلى التعريف المشترك والإطار المفاهيمي المتسق. ويستخدم ترسانة حية من المصطلحات، وتكون أحيانا فيكون على شكل تركيبة مع البادئات (Prefixes) مثل الإنترنت، والكمبيوتر، والبريد، والإنترنت، أو المعلومات الرقمية. حيث انتشرت هذه المصطلحات، وطبقت بشكل عشوائي، وهذا يعكس التداخل في المحتوى أو يعكس فجوات مهمة.

وهناك مقياس طور من قبل برنامج سايبر الجريمة الإلكترونية التابع للشرطة الهولندية (*Programma Aanpak Cybercrime*) فمن الواضح أنه في هولندا، هناك فروق ذات دلالة موجود في نطاق التعاريف المستخدمة للجريمة الإلكترونية، وفي أنواع الجريمة الإلكترونية التي تقع ضمنها والتي لا تقع ضمنها. وتتراوح التعريفات، على سبيل المثال، من: "أي نوع من الجريمة التي ترتبط بأنظمة الكمبيوتر والتي لا ترتبط بمعانيها، إلى كل جريمة ناتجة من استخدام المكون الرقمي (PAC, 2008, p.1). فمن الواضح أن هذه التعاريف تختلف إلى حد ما في طبيعتها. فالتعريف الأول تعريف ضيق: الجرائم التي ترتكب فقط على أنظمة الحاسب، على سبيل المثال، شملت القرصنة ونشر الفيروسات، في حين أن جرائم مثل الاحتيال والمطاردة عبر الإنترنت لم يشملها. أما التعريف الثاني فواسع : فشمل الجرائم التي استخدم الجاني فيها مجرد هاتف محمول أو نظام الملاحة عبر الأقمار الصناعية لارتكاب الجريمة.

ولقد عرفها ليوكفيلدت وفنسترا وستول (Leukfeldt, Veenstra & Stol, 2013)" " كمصطلح عام لجميع أشكال الجريمة التي تلعب فيها تكنولوجيا المعلومات والاتصالات (ICT) دوراً أساسي. وهنا تقع الكثير من الجرائم ضمن هذا التعريف. لقد قدم ليوكفيلدت وآخرون((Leukfeldt et al. (2012) قائمة ب ٢٨ جريمة بدءا من قرصنة الأنظمة الرقمية، وتثبيت برامج التجسس للاحتيال باستخدام الخدمات المصرفية عبر الإنترنت والمطاردة الافتراضية(Leukfeldt, Veenstra & Stol, 2013).

التعريف الدولي للجريمة الإلكترونية

- تعتمد "تعريفات" للجريمة الإلكترونية في الغالب على الغرض من استخدام المصطلح
- هناك عدد محدود من الأفعال ضد السرية والنزاهة وتوافر بيانات الكمبيوتر أو أنظمته تمثل جوهر الجريمة الإلكترونية

- أعمال متعلقة بالكمبيوتر لتحقيق مكاسب شخصية أو مالية أو ضرر، بما في ذلك أشكال الأفعال المتصلة بجريمة الهوية، وجرائم محتويات الكمبيوتر لا تصلح بسهولة إلى الجهود للوصول إلى التعاريف القانونية للمصطلح الكلي

بعض التعاريف تحتاج إلى جوهر أفعال الجريمة الإلكترونية، ومع ذلك، فإن أي 'تعريف' للجريمة الإلكترونية ليس ذا صلة لأغراض أخرى، مثل تعريف نطاق التحقيق المتخصص وقوى التعاون الدولي، والتي من الأفضل أن تركز على الأدلة الإلكترونية على بناء مفاهيمي عام ومصطنع هو الجريمة الإلكترونية. (UNODC, 2013, p. 11)

مصطلح " الجريمة الإلكترونية"

حاولت العديد من الأعمال الأكاديمية تعريف " الجريمة الإلكترونية"، ومع ذلك فلا تبدو التشريعات الوطنية، مهتمة بتعرف دقيق للمصطلح. فمن أصل حوالي ٢٠٠ مكون منبثقة من التشريعات الوطنية التي استشهدت بها البلدان في الرد على الاستبيان الدولي في تحديد معنى الجريمة الإلكترونية، أستخدم أقل من خمسة في المئة كلمة " جرائم الإلكترونية " في العنوان أو في السياق التشريعي وبدلا من ذلك فالاستخدام الأكثر شيوعاً في التشريعات هو لمصطلح "جرائم الكمبيوتر"، و"الاتصالات الإلكترونية"، و"تكنولوجيا المعلومات"، أو الجريمة ذات التقنية العالية. وفي الممارسة العملية ، فإن العديد من هذه المفردات من التشريعات التي إنشاؤها للجرائم الجنائية والتي هي المدرجة في مفهوم الجريمة الإلكترونية ، مثل الدخول غير المصرح به لنظام الكمبيوتر ، أو التدخل في نظام الكمبيوتر أو البيانات. حيث لم تستخدم التشريعات الوطنية على وجه التحديد مصطلح "الجريمة الإلكترونية" في عنوان فعل أو قانون (مثل " قانون الجرائم الإلكترونية ") ، ومن النادر أن يتضمن جزء التعريفات تعريف الجريمة، وعندما يضمن مصطلح" الجريمة الإلكترونية" كتعريف قانون كان التعريف العام له ببساطة باسم " الجرائم المشار إليها في هذه القانون. وبطريقة مماثلة، فأن عدد قليل جدا من الصكوك القانونية الدولية أو الإقليمية تعريف الجريمة الإلكترونية فلا اتفاقية مجلس أوروبا للجرائم الإلكترونية (Council of Europe Cybercrime Convention)، واتفاقية جامعة الدول العربية (League of Arab States Convention)، ولا مشروع اتفاقية الاتحاد الأفريقي(Draft African Union Convention)، على سبيل المثال ، تضمنت تعريفاً للجريمة الإلكترونية لأغراض الصك. لقد عرف اتفاقية كومنولث الدول المستقلة (The Commonwealth of Independent States

Agreement)، من دون استخدام مصطلح " جرائم الإلكترونية" فعرفت ' الجريمة المتصلة بمعلومات الحاسوب ' بأنها ' العمل الإجرامي الذي يستهدف معلومات الحاسوب (UNODC, 2013,)

هدف استعراض الصكوك الدولية والإقليمية في الدراسة الدولية إلى التوصل إلى سلة من السلوكيات التي تعني "الجريمة الإلكترونية"، ويظهر استعراض هذه الصكوك نهجين رئيسيين هما : (١) المصطلحات المستندة إلى **بيانات ' الكمبيوتر ' أو نظامه**، و(٢) المصطلحات المستندة إلى **البيانات المستندة "المعلومات" أو نظمها**، ويشير تحليل عناصر التعريفات إلى أنه يمكن اعتبار المصطلحات قابلة للتبديل إلى حد كبير. ويبين الشكل التالي العناصر مشتركة من هذه التعريفات . في حين تختلف التسميات، وعدد من المفاهيم الأساسية متناسقة.

الحاسوب/نظم المعلومات
• معدات أو أدوات مترابطة ومتصلة والتي تمكن الحاسب أو برامج المعلومات من العمل والمعالجة التلقائية لبيانات الحاسب/والمعلومات ووظائف الحاسوب المنطقية والرياضية والتخزين بما في ذلك الحاسوب ونظم المعلومات، المخزنة والمعالجة والاسترجاع والتحويل من خلال الحاسوب ونظم المعلومات بما في ذلك منشاة اتصالات او معدات بما في ذلك الإنترنت

الحاسوب/برامج المعلومات
• تعليمات بصيغة برمجة تمكن الحاسوب ونظم المعلومات من معالجة بيانات الحاسوب والمعلومات مكونة عملية أو وظيفه يمكن تنفيذها من قبل الحاسوب او نظم المعلومات

بيانات الحاسوب/المعلومات
• تمثيل للحقائق / برنامج المعلومات/المفاهيم في الالة على صيغة قابلة للقراءة مناسبة للمعالجة من خلال الحاسب أو برامج المعلومات أو الحاسوب/ نظم المعلومات بما في ذلك الحاسوب؟ برنامج المعلومات

شكل رقم (١)اتجاهات تعريف الجريمة الإلكترونية المصدر: (UNODC, 2013, p. 13)

الميزة الأساسية للأوصاف القانونية لل ' الحاسوب '، ' ونظام الحاسوب ' أو ' نظام المعلومات ' ، على سبيل المثال ، هو أن المعدات يجب أن يكون " قادرة على معالجة بيانات الحاسوب أو المعلومات. حددت بعض الأساليب إن المعالجة يجب أن تكون معالجة ' تلقائية ' أو "عالية السرعة "، أو عملاً للبرنامج. بعض

الاتجاهات وسعت تعريف المعدات إلى التي تقوم بالتخزين أو نقل وتلقي بيانات الحاسوب أو المعلومات، البعض أضاف للتعريف بيانات الحاسوب التي تتم معالجتها من قبل النظام. وحيث أن مصطلح " نظام الحاسوب " أو " نظام المعلومات " يستثني المعلومات المخزنة في النظام أو في أجهزة التخزين الأخرى، وغالبا ما يتم التعامل معها بشكل منفصل في الأحكام القانونية الموضوعية. في حين أن بعض الصكوك تعرف كل ' الحاسوب و " نظام الحاسوب "، وتضمن الأخير عادة السابق، وسياق استخدام كل المصطلحين دوم فرق بينهما في الممارسة (UNODC, 2013).

ومن الشائع وصف "بيانات الحاسوب" أو "معلومات الحاسوب" كتمثيل للحقائق، والمعلومات أو المفاهيم التي يمكن قراءتها ومعالجتها، أو تخزينها بواسطة الحاسوب. توضح 'بعض الاتجاهات أن هذا يشمل جهاز الحاسوب، والبعض الآخر التزم الصمت بشأن هذه النقطة. ومن المحتمل أن يكون الفرق ذا دلالة فقط بين بين تركيبات "المقروءة آليا" و "يمكن قراءتها ومعالجتها أو تخزينها بواسطة نظام الحاسوب (أو نظام المعلومات). ففي الممارسة العملية، من المرجح أن تتضمن بيانات الحاسوب أو المعلومات على وسائط التخزين المادية (مثل الأقراص الصلبة، و USB أو بطاقات فلاش للتخزين) أو البيانات أو المعلومات المخزنة في ذاكرة الحاسوب أو نظام بث نظام المعلومات أو البيانات أو المعلومات (سواء السلكية أو البصرية، أو تردد الراديو) ويعرض مادياً للبيانات أو المعلومات، مثل على شكل نسخة مطبوعة أو على شاشة الجهاز (UNODC, 2013).

ويمكن مقارنة بعض نماذج الجريمة التقليدية مع الجريمة الإلكترونية لنرى كيف انتقلت الجريمة من الواقع المادي إلى الواقع الافتراضي.

الجريمة التقليدية	الجريمة الإلكترونية
الاحتيال	الاحتيال على الشبكة، الاحتيال بالمزاد الإلكتروني....الخ
السطو	القرصنة على الإنترنت، الحرمان من الخدمة، الفيروسات
جرائم الأطفال الجنسية	استمالة الأطفال على النت، المواقع الإباحية
غسيل الأموال	أنظمة الدفع على الشبكة
السرقة	جرائم الهوية، وسرقة الملكية

.(Acc, 2013)

الأفعال التي تشكل جرائم الإنترنت

يبين الشكل أدناه ١٤ من الأفعال التي قد تشكل جرائم الإلكترونية، والتي نظمت في ثلاث فئات واسعة. ويتوافر في الدراسة الدولية مكتب الأمم المتحدة للمخدرات والجريمة ((UNODC, 20131)) ملحق يصف بتفاصيل عن كل فعل. وقد استخدمت هذه القائمة من الأفعال أيضا في الاستبيان الذي أرسل إلى

الدول، ومنظمات القطاع الخاص، والمنظمات الحكومية الدولية والمنظمات الأكاديمية لجمع المعلومات، والغرض من القائمة هو لإدخال مجموعة مبدئية من الأفعال التي يمكن أن تدرج في مصطلح " الجرائم الإلكترونية "، وذلك بهدف وضع أساس للتحليل خلال الدراسة. وليس المقصود من القائمة أن تكون شاملة. بالإضافة إلى ذلك، فالمصطلحات المستخدمة – والأوصاف المرفقة في الملحق واحدة – ولا يقصد منها أن تمثل التعاريف القانونية للجرائم الإلكترونية. بدلا من ذلك، فهي واسعة على وصف الأفعال " التي يمكن أن تستخدم بمثابة البداية في التحليل و المناقشة. (UNODC, 2013).

الافعال ضد السرية والنزاهة وتوافر بيانات الحاسب أو النظم

- الدخول غير المشروع لنظام الحاسوب
- الدخول غير المشروع، اعتراض أو الاستيلاء على بيانات الحاسوب
- الاستنتاج غير المشروع لبيانات الحاسوب أو نظامه
- إنتاج أو توزيع أو امتلاك لأدوات إساءة استعمال الحاسوب
- اختراق الخصوصية أو أساليب حماية البيانات

أفعال ذات الصلة بالحاسوب لمصالح شخصية أو مادية أو أذى

- الاحتيال المتعلق بالحاسوب أو التزوير
- جرائم الحاسوب ذات الصلة بالهوية
- حقوق الطبع والنشر أو جرائم العلامة التجارية ذات الصلة بالحاسوب
- إرسال أو السيطرة على إرسال البريد المزعج
- الأعمال ذات الصلة بأجهزة الحاسوب الشخصية التي تسبب الضرر
- الإغراء أو استمالة الأطفال المتعلق بالحاسوب

الأفعال ذات الصلة بمحتويات الحاسوب

- الأفعال ذات الصلة بالحاسوب التي تنطوي خطاب الكراهية
- الإنتاج أو توزيع أو حيازة المواد الإباحية عن الأطفال المتعلقة بالحاسوب

- الأعمال ذات الصلة بأجهزة الكمبيوتر في دعم جرائم الإرهاب (UNODC, 2013).

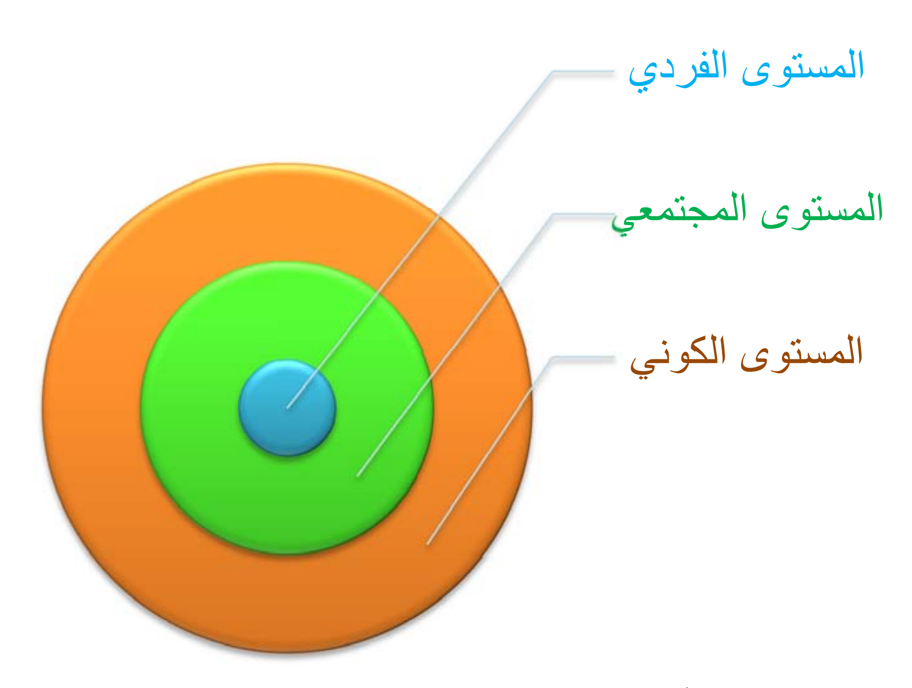
حجم مشكلة الجرائم الإلكترونية:

هناك حوالي ٨٠ % من أعمال الجريمة الإلكترونية تنشأ في شكل من أشكال النشاط المنظم، مع سوق الجرائم الإلكترونية الأسود، على شكل عمل دورة البرمجيات الخبيثة، وفيروسات الكمبيوتر، وإدارة الروبوتات، وحصاد البيانات المالية، وبيع البيانات، وقبض ثمن المعلومات المالية. لم يعد يحتاج مجرمو الجرائم الإلكترونية مهارات أو تقنيات معقدة.

على الصعيد العالمي، تظهر أفعال الجريمة الإلكترونية انتشاراً واسعاً عبر أعمال مدفوعة ماليا، وأعمال ذات صلة بمحتوى الكمبيوتر، وكذلك العمل ضد السرية والسلامة والوصول إلى أنظمة الكمبيوتر. تختلف تصورات المخاطر والتهديد النسبي، بين الحكومات ومؤسسات القطاع الخاص. حاليا، لا تمثل إحصاءات الجريمة المسجلة لدى الشرطة أساسا سليما لإجراء مقارنات عبر الوطنية، على الرغم من أن هذه الإحصاءات غالبا ما تكون هامة لرسم السياسات على المستوى الوطني. يرى ثلثي الدول أن أنظمتها غير كافيه لإحصاءات الشرطة في تسجيل الجريمة الإلكترونية. وترتبط سجلات الشرطة للجريمة الإلكترونية مع مستويات الدولة التنموية وقدرة الشرطة المتخصصة (UNODC, 2013).

أسباب الجريمة الإلكترونية

هناك عدد من الأسباب التي يمكن حصرها كأسباب للجريمة الإلكترونية، منها ما يقع على مستوى كوني، ومنها ما يقع على مستوى مجتمعي، ومنها ما يقع على مستوى فردي أو شخصي. كما ان أسباب الجريمة الإلكترونية تتفاوت وفق نوعها ونوع المستهدف ونوع الجاني ومستوى تنفيذه (فردي، مجتمعي ، كوني). فجرائم الشباب والهواه والصغار تختلف عن أسباب جرائم المحترفين، وتختلف وفق هدفها سرقة أو معلومات أو تجارة بالمعلومات أو شخصية....الخ.



شكل رقم (٢) أسباب الجريمة الإلكترونية وفق مستوى التحليل

أسباب الجريمة على المستوى الفردي.

البحث عن التقدير (sake of recognition)

هناك بعض الجرائم الإلكترونية التي يرتكبها شباب طائش وصغار سن، وذلك من باب التحدي، وحب الظهور في الإعلام. وغالباً ما تتوقف هذه الفئة عن مثل هذه السلوكيات في عمر لاحق بعد سن العشرينيات.

الفرصة (Opportunity). لقد وفرت التقنيات الحديثة والأنترنت فرصاً غير مسبوقة لانتشار الجريمة الإلكترونية. أنّ الفرصة تنتج الجريمة (Felson & Clark, 1998). وتلعب البيئة وترتيباتها دوراً كبيراً في إنتاج الجريمة، والخروج على قواعد الاجتماعية. فوقت الانحراف عن قواعد الامتثال ليلاً ونهاراً وفي اي مكان، وعدم وجود رقابة، كلها عوامل تزيد من فرصة ارتكاب الجريمة الإلكترونية. وقد تشكل المعلومات هدفاً سهل المنال، ويحقق المنفعة السريعة، وبالتالي يمكن سرقتها، أو سرقة محتوياتها. فهي فرصة مربحة، وقليلة المخاطر، واحتمالية الكشف للفاعل فيها ضئيلة (Rice & Smith, 2002).

أن تكنولوجيا المعلومات والاتصالات والاستخدام المتزايد للأنترنت قد خلق **فرص جديدة للمجرمين** وسهلت نمو الجريمة. أن جرائم الإنترنت تمثل "شكلا جديداً ومميزاً للجريمة، وقد خلقت تحديات لتوقع التطورات، والوقاية منها، (UNODC, 2013).

ضبط الذات المنخفض. تنطلق هذه الدراسة من النظرية العامة في السلوك الطائش (Gottfredson & Hirschi, 1990) . وتؤكد هذه النظرية أن احتمالية انخراط الأفراد في فعل إجرامي تحدث بسبب وجود الفرصة مع توفر سمة شخصية من سمات الضبط الذاتي المنخفض. وقد عرف كل من جتفردستون وهيرشي السلوك الطائش بأنّه: كل فعل يقوم على القوّة والخداع لتحقيق الرغبات الذاتية. وبناء على هذا التعريف الذي يستدل على طبيعة السلوك الطائش من خصائص الأشخاص، فإن السلوك الطائش يُعدّ مظهراً من مظاهر الضبط الذاتي المنخفض، وكما في نظرية الضبط الاجتماعي لهيرشي ، فالدوافع لارتكاب السلوك الطائش ليست متغيرة. وذلك لأن كل فرد قد يندفع لتحقيق مصالحه الشخصية بما في ذلك السلوك الطائش. فالسلوك الطائش يُعدّ عملاً سهلاً وقد يحقِق المصالح الخاصة بسرعة مثل (الرشوة، السرقة) ونحوهما من الأعمال الإجرامية التي تتحقق بسرعة وسهولة دون انتظارٍ أو بذل جهد، ولكن الاختلاف بين الأفراد يعود إلى مستوى ضبط الذات، ووجود الفرصة لارتكاب السلوك المنحرف(البداينة والرشيد والمهيزع، ٢٠٠٥).

إن توفر صفة الضبط الذاتي المنخفض مع وجود الفرصة لارتكاب السلوك الطائش يعدان عاملين مؤثّرين في ارتكاب السلوك الطائش، فتأثير هذين العاملين يكون نتيجة لاتحادهما، والتفاعل بينهما هو المؤدّي للسلوك الطائش. وقد حاول كلّ جتفردستون وهيرشي عزو الاختلاف بين المجرمين وغيرهم إلى الاختلافات في مستوى ضبط الذات. إن نقص ضبط الذات قوة طبيعية تظهر في غياب الخطوات من أجل تطويره، أي أنه نتاج للتنشئة الاجتماعية الناقصة، حيث يفشل الآباء في مراقبة سلوك الطفل، ولا يلاحظون السلوك المنحرف عندما يحدث، وإهمال معاقبة الطفل عندما يقترف سلوكاً منحرفاً. وعندما يتكوّن الضبط الذاتي في المراحل الأولى عند الأفراد، فإن الاختلافات في ضبط الذات تبقى ثابتة بشكل معقول من الوقت الذي تم تحديده عبر أطوار الحياة غير متأثر بالمؤسسات الاجتماعية (البداينة والرشيد والمهيزع، ٢٠٠٥). بل على العكس فإن ضبط الذات قد يؤثر على أداء الأفراد في هذه المؤسسات، مثل المدرسة والعمل

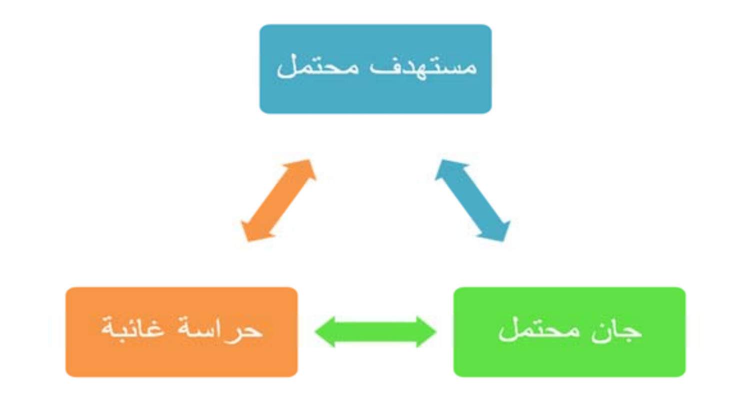
والزواج. والأشخاص ذوو الضبط المنخفض لا يميلون إلى السلوكيات المنحرفة فقط، بل إنهم في الأغلب غير ناجحين في المدرسة أو العمل أو الزواج (البداينة والتوايهة، ٢٠١٠)

أظهرت الدراسات أيضا أن ضبط الذات المنخفض والاستعداد لتحمل المخاطر من أجل تحقيق مكاسب قصيرة الأجل، وهذا قد ينطبق على الأفعال التي يمكن إن تسهيل أو تتعزز بواسطة وسائط الاتصالات الإلكترونية والإنترنت. بالإضافة إلى ذلك، يتعرض الأفراد على الإنترنت لنماذج التعلم الإجرامي والأقران قد يكونون أكثر ميلا للانخراط في الجريمة الإلكترونية. ونظرية التعلم الاجتماعي " نظرية قد يكون لها تطبيق خاص عندما يتعلق الأمر بالجرائم الإلكترونية ، فالمجرمين غالبا ما تحتاجون إلى تعلم تقنيات الكمبيوتر والإجراءات. فالنظرية العامة للجريمة ونظرية التعلم الاجتماعي، تريان إن الأفراد يتصرفون في البيئة الافتراضية كما يتصرفون في العالم الحقيقي.

الضغوط العامة (General Strain). ترجع نظرية الضغوط العامة الانحراف وخرق القانون إلى دافع ناجم عن قوى البناء الاجتماعي أو استجاباته النفس اجتماعية للحوادث والظروف والتي تعمل كضغوطات أو مقلقات خاصة عندما لا تتاح للأفراد الفرصة لتحقيق أهدافهم المقبولة اجتماعياً (Merton, 1938; Agnew, 1992)، وأن مصادر الضغوط لا تتوقف على الإحباط الذي يخبره الفرد عندما تُسد الطرق لتحقيق هدف ما، وإنما يشمل المشاعر السلبية التي تحدث في المواقف الاجتماعية المتنوعة (Paternoster & Mazerolle, 1994). **كما** قد تلعب العوامل الاجتماعية والاقتصادية أيضا دورا هاما في زيادة الجريمة الإلكترونية. فالضغط على مؤسسات القطاع الخاص لخفض الإنفاق وخفض مستويات التوظيف يمكن أن يؤدي، على سبيل المثال، إلى تخفيضات في الأمن، وإلى فرص لاستغلال ثغرات وضعف تكنولوجيا المعلومات والاتصالات والشركات. مما يضطر لتوظيف المتعاقدين من الخارج أو المؤقتين، أو يصبح هناك موظفين ساخطين بسبب انخفاض الأجور والخوف من فقدان الوظيفة، والخطر يزداد من الأعمال الإجرامية والنفوذ من قبل منظمة إجرامية (UNODC, 2013).

النشاط الروتيني. ويمكن تفسير زيادة ضحاي الجريمة الإلكترونية من خلال التغييرات في أنشطة الناس الروتينية في الحياة اليومية. فمع ظهور شبكة الإنترنت فقد تغيرت طريقة الناس التي يتواصلون فيهها أو يتفاعلون مع الآخرين في العلاقات الشخصية، والترفيه، والتجارة...الخ . أن التغيرات في أنشطة الناس الروتينية، من مثل استخدام النت وشبكات التفاعل الاجتماعي مثل الفيس بوك، والايميل والمواقع وغيرها قد

خلقت فرصاً للجناة المتحفزين مع وجود أهداف قيمة وسهلة في الحيز الفضائي مع غياب الحراسة. يرى كوهين و فيلسون (Cohen and Felson, 1979) إلى أنه من المرجح أن تحدث الجريمة عندما تتلاقى ثلاثة عوامل هي: هذه العوامل هي: الجاني المتحفز (Motivated offender) والهدف المناسب (suitable targets) وغياب الحراسة (absence of capable guardians).



شكل رقم (٣) نظرية الفرصة المصدر : البداينة وآخرون، ٢٠٠٩

أنه لا بد من توافر هذه العوامل الثلاثة من أجل أن تحدث الجريمة، وعدم وجود واحد من هذه العوامل هو " كافي لمنع حدوث ناجح لإكمال الاتصال المباشر في جريمة السلب (Cohen and Felson, 1979 P. 589) ويعطي اهتمام إلى التقارب في الزمان والمكان، وإن هذا التلاقي يمكن أن يؤدي إلى زيادة كبيرة في معدلات الجريمة من دون أي تغيير في " الحالة الظرفية" التي تحفز المجرمين (Cohen and Felson, 1979). المبدأ الأساسي هو أن التغييرات الهيكلية في النشاط الروتيني تؤثر على التقارب في العناصر الثلاثة من الناحية النظرية، وبالتالي تؤثر على معدل الجريمة (Meithe, Mark, and Scott, 1987).

يبين الشكل أدناه، عناصر النظرية الثلاثة الرئيسة في العالم الافتراضي في الجريمة الإلكترونية، حيث الجاني المتحفز (قد يكون) والمستهدف المناسب (استهداف الهوية أو المال)، ولكن الحراسة القادرة (برامج الحماية وبرامج المضادة للفيروسات).



شكل رقم (٤) سياق الجريمة الإلكترونية وفق النشاط الرتيب
Adapted from Felson, Marcus. (2002). Crime and Everyday Life, p. 33

أسباب الجريمة على المستوى المجتمعي

التحضر(Urbanization). يعد التحضر أحد أسباب الجريمة الإلكترونية عامة، حيث الهجرة الكبيرة من الريف إلى المدينة وإلى المناطق الحضرية والمدن الكبيرة. وعادة ما يهاجر الشباب غير المتمكنين من مواجهة متطلبات الحياة الحضرية، باهضه التكاليف، والتي تتطلب مهارات عالية أحيانا. مما يجعل شرائح كبيرة من المهاجرين غير قادرين على تلبية متطلبات الحياة الحضرية، مما يجعلهم يعيشون في مدن الصفيح والأحياء الطرفية والهامشية. وكنتيجة يجد الناس انفسهم في تنافس غير قادرين على مجاراته، مما يجعلهم يلتفتون إلى الاستثمار في الجريمة الإلكترونية حيث لا تتطلب راس مال كبير والتي تعرف "أولا الياهو" (Yahoo Boys). وكما يرى ميك (Meke, 2012). فأن التحضر سبب رئيس للجرائم الإلكترونية في نيجيريا، وان التحضر بدون الجريمة مستحيل، وكنتيجة فان الصفوة بينهم قد وجدوا إن الاستثمار في الجريمة الإلكترونية مربحة (lucrative).

البطالة(Unemployment). ترتبط الجريمة الإلكترونية شأنها شأن الجريمة التقليدية بالبطالة والظروف الاقتصادية الصعبة. وتتركز البطالة بين قطاعات كبيرة من الشباب. وكما يقول المثل النيجيري "العقل

العاطل عن العمل هو ورشة عمل للشيطان" ولذا فان الشباب الذين يملكون المعرفة والمعرة سيستثمرون ذلك في النشاط الإجرامي الإلكتروني.

الضغوط العامة (Strains). تعد الضغوط العامة التي يتعرض لها المجتمع من فقر وبطالة وأمية وظروف اقتصادية صعبة عوامل ضاغطة على المجتمع عامة وخاصة على قطاع الشباب، مما يولد مشاعر سلبية عند شرائح كبيرة من الناس ضد الظروف وضد المجتمع مما يدفعهم إلى أساليب تأقلم سلبية مع هذه الظروف منها الإتجار الإلكتروني بالبشر والجنس والجريمة الإلكترونية وغيرها.

البحث عن الثراء(Quest for Wealth). يسعى الأنسان إلى المتعة ويتجنب الألم هكذا تقول النظرية العامة في الجريمة لجتفردسون وهيرشي (Gottfredson and Hirschi, 1990)، ويسعى الناس إلى الوسائل غير المقبولة اجتماعيا لتحقيق أهداف مقبولة اجتماعيا كما ترى نظرية الأنومي لميرتون. فالرغبة في الثراء يواجها صعوبات بالغة في تحقيقه بالطرق المقبولة اجتماعيا والقانونية، ولذا يلجأ بعض الناس إلى الجرائم الإلكترونية حيث المستهدف مجتمع أكبر وسهولة التنفيذ وسرعة المردود وقلة الخطورة.

ضعف إنفاذ القانون وتطبيقه في الجريمة الإلكترونية (lack of law enforcement and implementation). هناك الكثير من الدول التي لم تطور تشريعاتها وأجهزة العدالة فيها لكي تتمكن من مجاراة التقدم في الجرائم الإلكترونية وأساليبها. وهذا لا يتوقف عند التشريعات وإنما يشمل الشرطة والتحقيق والقضاء، وكيفية التعامل مع الأدلة الرقمية على المستوى الوطني، كما هو الحالي على المستوى الدولي. فمما يشعل الجريمة الإلكترونية غياب التشريعات الجزائية والجنائية وضعف الممارسات العدلية والشرطية والقضائية في محاكمة والتحقيق في الجرائم الإلكترونية. وغالباً ما تجد في دول كثيرة تواضع التقنيات المتوافرة وكذلك الخبراء القادرون على متابعة ورصد وملاحقة الجريمة الإلكترونية داخل المجتمع والعابرة منها للحدود الوطنية.

أسباب الجريمة على المستوى الكوني.

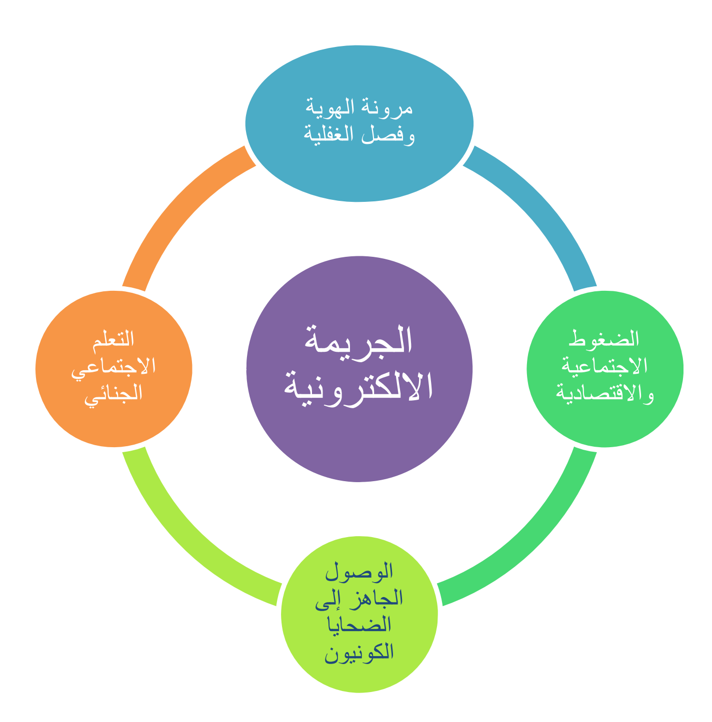
التحول للمجتمع الرقمي. إن من أهم سمات عصر المعلومات السمات الثلاثة الرئيسة : (١) تغيرات كمية في مقدار المعلومات المتدفقة ونوعيها، فبفعل تكنولوجيا الاتصالات والمواصلات فأن الصور والمعلومات تغطي كافة المعمورة بسرعة ودقة. (٢) إرسال المعلومات إلى العديد من الأطراف (البشر والمعدات) فالمعلومات توجه الصاروخ والصحفي يرسل التقرير، والبث المباشر من مكان الحدث. (٣) وجود الشبكات (Networking) حيث يتم تداول المعلومات بين جميع الأطراف من مثل البريد الإلكتروني، الجوال، ... الخ (كوهين،٢٠٠١) (البداينة، ٢٠٠٨). ففي الفضاء الافتراضي، تكونت التفاعلات الافتراضية وحلت محل

التفاعل وجها لوجه وتكونت السلوكيات الافتراضية والشخصية الافتراضية والمجتمع المحلي الافتراضي. (Al-badayneh, 2012).

لقد دخلنا عصر المعلوماتية الجديدة (أي الفضاء الإلكتروني أو العالم الافتراضي). فالناس يقضون جزءا من حياتهم اليومية في الفضاء الإلكتروني، ينشؤون الشبكات والمواقع ويتمتعون بأنواع جديدة من العلاقات الاجتماعية، وهم على تواصل مع ما يجري في العالم الخارجي، والقيام ببعض الأعمال. كل من هذه الأنشطة قد جعلت من الممكن للجميع وبوجود جهاز كمبيوتر أو مودوم مع معرفة التقنية القليلة. وبعبارة أخرى ، فإن شبكة الإنترنت هي من خلقت ما يعرف الآن باسم الفضاء الإلكتروني، أو العالم الافتراض. يحتاج المجتمع لكي يقوم بوظائفه إلى أن يعم الأمن والأمان وان يتحقق النظام والاستمرارية. ولا يتوقف توفر الأمن والأمان في الواقع المادي للمجتمع بل أنتقل ليشمل العالم الافتراضي(cyber space)(Stol, 2008, Leukfeld, Vennstra, and Stol, 2013).

العولمة

أن ظهور "الفضاء الإلكتروني" يخلق ظواهر جديدة متميزة عن وجود أنظمة الكمبيوتر أنفسها، والفرص المباشرة للجريمة والتي وفرتها أجهزة الكمبيوتر الآن. ضمن الفضاء الإلكتروني، قد يظهر الأشخاص الفروق في امتثالهم الخاص (القانوني) وعدم الامتثال (غير القانوني) مقارنة مع السلوك سلوكهم في العالم المادي. فالأشخاص، على سبيل المثال، قد يرتكبون جرائم في الفضاء الإلكتروني لا يرتكبونها في الواقع المادي بسبب مكانتهم وموقعهم. بالإضافة إلى ذلك، فمرونة الهوية (identity flexibility)، وعدم ظهور الهوية وضعف عوامل الردع تحفز السلوك الإجرامي في العالم الافتراضي(UNODC, 2013).



UNODC, 2013, p. 8

شكل رقم (٥) تصور لبعض أسباب الجريمة الإلكترونية في الفضاء التخيلي

هذا العصر يتطلب مؤسسات أمنية مصممة للتعامل مع التغير السريع، تركز على الإبداع والشفافية وإرضاء العملاء (المجتمع بأسره)، مؤسسات ذات سرعة عالية في نشر المعلومات وأعلام الجمهور. مؤسسات قادرة على إعادة تصميم ذاتها (الهندرة re-engineering) لمواجهة المستجدات السريعة والسريعة التغير في عالم الجريمة الإلكترونية. (البداينة، ٢٠٠٤).

الترابط الكوني. وهناك عامل يمكن أن يساهم في دفع مستويات الجريمة هو في ظهور الترابط العالمي في سياق تحولات العالم الاقتصادية والديموغرافية. بحلول عام ٢٠٥٠ ، فإن العالم سوف يشهد تضاعف عدد سكان الحضر إلى ٦.٢ مليار – ٧٠ في المائة من سكان العالم المتوقع من ٨.٩ مليار. UNODC, (2013). أكد تقرير صدر عن المركز الوطني لجريمة الياقات البيضاء(national White Collar Crime center NW3C, 2002) (2002) (NW3C) يؤكد أن فضاء الإنترنت قد خلق فرصا جديدة للمجرمين في التواصل مع الضحايا. هو وقد بين أن السمات الفريدة للإنترنت، وهي عدم الكشف عن اسم الشخص وسهولة الاستخدام، قد وفرت طرق جديدة للمجرمين لارتكاب جرائمهم. بالإضافة إلى ذلك، يتيح الإنترنت للمجرمين على التواصل بسرعة و بكفاءة نقل كميات كبيرة من المعلومات إلى العديد من الضحايا عبر غرف الدردشة، والبريد الإلكتروني، ولوحات الرسائل، أو مواقع ويب (NW3c, 2002). وكل الذي

يحتاجونه هو مهارات الحاسوب الأساسية و أجهزة الكمبيوتر المتصلة بالإنترنت. .وبناء على ذلك يوفر جهاز كمبيوتر واحد وسائل متنوعة لإجراء مجموعة من الجرائم. ويمكن للمجرمين استخدام الكمبيوتر لبدء تواصل مع الضحايا وإدامته عن طريق شبكة الإنترنت، لإجراء المعاملات المالية الاحتيالية (NW3C, 2002). يشير، في مخططات المصرفية على الإنترنت المجرمين جمع المعلومات الشخصية السرية ب " انتحال موقع ويب صحيحة، إنشاء موقع ويب الخادعة ، أو حتى يروج المشروعة السبر احتيال في غرفة دردشة " . عندما يحصل مجرم معلومات الحساب المصرفي ، التحويلات غير المشروعة من المال ، على سبيل المثال ، يمكن أن يحدث في واحدة الصفقة السريع(NW3C) .

انكشاف البنية التحتية المعلوماتية الكونية

تتفاوت البني التحتية المعلوماتية بدرجة انكشافها إلى الكوارث الطبيعية، والإهمال البشري، وسوء التصرف الإنساني. حدد التقرير الرئاسي الأمريكي بخصوص حماية البنية التحتية الحساسة (PCCIP, 1997) خمسة قطاعات بناءً على الخصائص المشتركة لها، وهذه القطاعات هي :

١. قطاع الاتصالات والمعلومات (Information and Communication)، وتشمل شبكات الاتصالات العامة (PTN)، والإنترنت، والحاسبات في المنازل، والاستخدام الأكاديمي، والحكومي، والتجاري.
٢. قطاع التوزيع المادي (الفيزيقي) (Physical Distribution)، ويشمل الطرق السريعة للمواصلات، وخطوط السكك الحديدية، والموانئ، وخطوط المياه، والمطارات، وشركات النقل، وخدمات الشحن التي تسهل انتقال الأفراد والبضائع.
٣. قطاع الطاقة (Energy)، وتشمل الصناعات التي تنتج الطاقة، وتوزع الطاقة الكهربائية، والبترول، والغاز الطبيعي.
٤. قطاع المال والبنوك (Banking and Finance)، وتشمل البنوك، وشركات الخدمات المالية من غير البنوك، ونظم الرواتب، وشركات الاستثمار، والقروض المتبادلة، والتبادلات الأمنية والمادية.
٥. قطاع الخدمات الإنسانية الحيوية (Vital Human Services)، وتشمل نظم التزويد بالمياه، وخدمات الطوارئ والخدمات الحكومية (البطالة، والضمان الاجتماعي، وتعويض الإعاقات، وإدارة سجلات المواليد ... الخ.).

من الصعب ربط التهديدات الإلكترونية بمكان أو زمان، أو جماعة، فقد تصدر من هاو أو من طفل أو محترف، أو جماعة إرهابية، أو جماعة تنافسية، أو استخبارات أجنبية. ولقد حددت وكالة مشاريع البحوث الدفاعية المتقدمة (DARPA) مهددات البناء التحتي ألمعلوماتي في (٥) فئات.

١. التهديدات الخارجية المحايدة (External Passive Attack) [التنصت، وتحليل الإشارات، وتحليل الذروة].
٢. التهديدات الخارجية النشطة (External Active Attack)، [مثل الدخول، والحمولة الزائدة، والازدحام].
٣. الهجوم على نظام عامل (Running System Attack).
٤. الهجوم الداخلي (Internal Attack).
٥. الهجمات للوصول إلى تعديل النظام [خرق حماية الدخول للنظم، الانكشاف]

(موثق في البداينة ٢٠٠٢)(DARPA, 1997, Appendix C).

أسباب تتعلق بخصائص الجريمة الإلكترونية

فيما يلي مجموعة من خصائص الجرائم الإلكترونية والتي تؤدي إلى ارتكاب الجريمة الإلكترونية منها:

١. **الازالة (Removable)**. الجريمة الإلكترونية لا تتطلب الإزالة فيمكن نسخها فقط.
٢. **التوافر (Available)**. المعلومات في كل مكان، جاهزة لتستدف من الجريمة
٣. **القيمة (Valuable)**. معلومات بطاقات الائتمان والحسابات المصرفية والتصاميم... قيمة
٤. **المتعة (Enjoyable)**. كثير من الجرائم الإلكترونية ممتعة من مثل سرقة الموسيقى والمال.
٥. **الديمومة (Durable)**. المعدات والبرامج المسروقة يمكن أن تستخدم لفترة طويلة.
٦. **سرعة التنفيذ:** لا يتطلب تنفيذ الجريمة الإلكترونية الوقت الكثير وبضغطة واحدة على لوحة المفاتيح يمكن أن تنتقل ملايين الدولارات من مكان إلى آخر. وهذا لا يعنى أنها لا تتطلب الإعداد قبل التنفيذ أو استخدام معدات وبرامج معينة.
٧. **التنفيذ عن بعد:** لا تتطلب الجريمة الإلكترونية في أغلبها (إلا جرائم سرقة معدات الحاسب) وجود الفاعل في مكان الجريمة. بل يمكن للفاعل تنفيذ جريمته وهو في دولة بعيدة كل البعد عن مكان الجريمة سواء كان من خلال الدخول للشبكة المعنية أو اعتراض عملية تحويل مالية أو سرقة معلومات هامة أو تخريب. الخ.

٨. **إخفاء الجريمة:** إن الجرائم التي تقع على الحاسبات الآلية أو بواسطتها (كجرائم الإنترنت) جرائم مخيفة، إلا أنه تلاحظ آثارها والتخمين بوقوعها.

٩. **الجاذبية:** نظراً لما تمثله سوق المعلومات والحاسب والإنترنت من ثروة كبيرة للمجرمين أو للإجرام المنظم، فقد غدت أكثر جذباً لاستثمار الأموال وغسيلها وتوظيف الكثير منها في تطوير تقنيات وأساليب تمكن الدخول إلى الشبكات وسرقة المعلومات وبيعها أو سرقة البنوك أو اعتراض العمليات المالية وتحويل مسارها أو استخدام أرقام البطاقات. إلخ.

١٠. **عابرة للحدود الدولية** (Transnational): إن ربط العالم بشبكة من الاتصالات من خلال الأقمار الصناعية والفضائيات والإنترنت جعل الانتشار الثقافي وعولمة الثقافة والجريمة أمراً ممكناً وشائعاً، لا يعترف بالحدود الإقليمية للدول، ولا بالمكان، ولا بالزمان، أصبحت ساحتها العالم أجمع (البداينة، ١٩٩٨ "ج"). (البداينة، ١٩٩٩ "د").

١١. **جرائم ناعمة:** تتطلب الجريمة التقليدية استخدام الأدوات والعنف أحياناً كما في جرائم الإرهاب والمخدرات، والسرقة والسطو المسلح. إلا أن الجريمة الإلكترونية تمتاز بأنها جرائم ناعمة لا تتطلب عنفاً، فنقل بيانات من حاسب إلى آخر أو السطو الإلكتروني على أرصدة بنك ما لا يتطلب أي عنف أو تبادل إطلاق نار مع رجال الأمن (سليم، ١٩٩٧).

١٢. **صعوبة إثباتها:** تتميز الجريمة الإلكترونية عن الجرائم التقليدية بأنها صعبة الإثبات، وهذا راجع إلى افتقاد وجود الآثار التقليدية للجريمة، وغياب الدليل الفيزيقي (بصمات، تخريب، شواهد مادية) وسهولة محو الدليل أو تدميره في زمن متناه القصر، يضاف إلى ذلك نقص خبرة الشرطة والنظام العدلي، وعدم كفاية القوانين القائمة (البحر، ١٩٩٩).

تصنيف مرتكبو الجرائم الإلكترونية

- **المثاليين(Idealists) (المراهقين)**. وعادة ما يكونون غير مدربين أو مهرة ، وهم الشباب الذين تتراوح أعمارهم بين ١٣-٢٦ والذين يسعون إلى الاعتراف الاجتماعي. وهم يريدون أن يكونون في بؤرة الضوء في وسائل الإعلام. وتمتاز أفعالهم بانها تسبب الخراب عالمياً ولكنها لا تذكر على المستوى الفردي. من "مثل الحرمان الكثير من خوادم هامة في التجارة الإلكترونية في شهر فبراير عام ٢٠٠٠ والتي سببت أضرار عالية لهذه الشركات. " وفي معظم الأحيان يهاجم المثاليون أنظمة المعلومات بفيروسات طوروها؛ وضررهم الفعلي على كل فرد لا يكاد يذكر. وعادة ما يتوقفون في سن ٢٦-٢٦ عندما ينضجون ويفهمون نتائج أعمالهم.

- **الجشع- المدفوع** (Greed-motivated) (المجرمون المهنيون). وهذا النوع من مجرمي الإنترنت خطير، وهذه الفئة عادة ما تكون عديمة الضمير وهم على استعداد لارتكاب أي نوع من الجرائم، طالما أنها تجلب لهم المال. حيث "بدأوا في إنتاج المواد الإباحية وغالبا ما تسمى السيبرانية للمواد الإباحية والتي تشمل الإباحية القانونية وغير القانونية على شبكة الإنترنت. " أنهم عادة ما يكونوا أذكياء جدا ومنظمون ويعرفون كيفية الهروب من وكالات إنفاذ القانون. ومجرمو الإنترنت هؤلاء يرتكبون الجرائم الخطيرة، وخاصة في جرائم إباحية الأطفال والقمار الإلكتروني وهذه تشكل تهديدا خطيرا للمجتمع.
- **الافتراضي- الإرهابيون** (The Cyber-terrorists) . هم مجموعة الأحدث والأكثر خطورة. والدافع الأساسي لهم ليس المال فقط ولكن أيضا لديهم قضية ما والتي يدافعون عنها. وعادة ما ينغمسون في إرسال رسائل التهديد وتدمير البيانات المخزنة في الغالب في نظم المعلومات الحكومية لمجرد أن يسجلوا وجهة نظرهم. ويمكن مقارنة تهديد الإرهاب الإلكتروني بتهديدات السلاح النووي، والبكتريولوجية أو الكيميائية. هذه المسألة المثبطة للهمم هي أنهم لا يعملون داخل حدود الدولة ؛ بل يمكن أن يعملوا من أي مكان في العالم، و هذا يجعل من الصعب اقتناصهم(Chizoba, 2005) .

ففي مجال الإرهاب أظهرت دراسة سالم وريد وشين (Salem, Reid, and Chen, 2008) والتي درسوا فيها محتوى فيديوهات للجماعات المتطرفة الإرهابية باستخدام تحليل المحتوى وأدوات الترميز في الوسائط المتعددة لاستطلاع وتحليل أنماط الفيديوهات وطريقة العمل (modus operandi) وخصائص المنتج الذي قاد إلى دعم هذه الجماعات المتطرفة. أظهرت الدراسة إن هذه الفيديوهات قد مررت رسائل قوية وكافيه لتعبئة الأفراد (mobilize) والمتعاطفين وحتى لتنفيذ هجمات مثل التي يحويها الفيديو ونشرها عالميا من خلال النت. وهذه الفيديوهات مهمة للجماعات الجهادية في مجالات التعلم والتدريب والتجنيد. بالإضافة إن جمع هذه الفيديوهات وتحليلها مفيد لصناع القرار ومحللي الاستخبارات، والباحثين في فهم أفضل حملات الإرهاب للجماعات المتطرفة وطرق عملها. كما أنها تساعد في استراتيجيات مكافحة الإرهاب وفي تدريب تكتيكات للجيش. ويظهر الجدول التالي تحليل لهذه الفيديوهات.

جدول (١) فيديوهات الشبكة المظلمة

نوع الفيديو	عدد الفيديوهات	الحجم (MB)	مدة التشغيل (hh:mm:ss)
وثائقي	291	2376.91	35:15:31
هجوم انتحاري	22	122.85	02:09:13
قطع رأس (beheading)	70	294.95	04:44:03
أخذ رهائن	26	172.8	02:24:13
جزية (Tribute)	13	128.69	02:49:40
رسالة	126	1293.91	44:60:48
دعاية	143	1566.98	23:42:19
تعليمات	1	16.72	00:08:24
تدريب	9	196.49	03:20:12
نشرة إخبارية	5	533.54	02:36:30
المجموع	7006	6723.83	122:06:53
المتوسط	**حجم الملف**	**مدة التشغيل**	**معدل البث**
	9.5MB	10.23	247.3kbps

المصدر: (Salem, Reid, and Chen, 2008, p.611) (موثق في البداينة، ٢٠١٣)

لقد كان متوسط مدة الفيديو في ال ٦٠ فيديو جهادي ٦:٣٢ دقيقة. أظهر التحليل وجود نوعين من الفيديوهات: **الفيديوهات العنيفة** وتتضمن الفيديوهات الوثائقية، والهجمات الانتحارية، وقطع الرأس والاختطاف. التي تستخدم لدعم الحرب النفسية للجهاديين واستراتيجيات التعبئة. **والفيديوهات الأخرى** وتتضمن الجزية، والفدية، والرسائل، والدعاية، والنشرات الإخبارية، ومحتويات خاصة من مثل أسماء المجموعات وعمل المجموعات (مثل التكتيكات والمستهدفون والأسلحة) والتي تمكن الجماعات المتطرفة من (أ) تعميم افتعالهم إلى مجتمعات متنوعة من الداعمين والمتعاطفين وجماعات الإعلام والأعداء (ب) ادعاء تحمل المسؤولية، (ج) نشر رسائلهم عالميا للحصول على الشرعية لأعمالهم.

أهم طرق الجريمة الإلكترونية:

وتشمل وليس حصرا على:

١. **تخريب المعلومات وإساءة استخدامها.** ويشمل ذلك قواعد المعلومات، المكتبات، تمزيق الكتب، تحريف المعلومات، تحريف السجلات الرسمية. الخ.

٢. **سرقة المعلومات** ويشمل بيع المعلومات كالبحوث أو الدراسات الهامة أو ذات العلاقة بالتطوير التقني، أو الصناعي، أو العسكري، أو تخريبها، أو تدميرها. الخ.

٣. **تزوير المعلومات** ويشمل الدخول لقواعد في النظام التعليمي وتغيير المعلومات وتحريفها، مثل تغيير علامات الطلاب.

٤. **تزييف المعلومات** وتشمل تغيير في المعلومات على وضع غير حقيقي مثل وضع سجلات شهادات لم تصدر عن النظام التعليمي وإصدارها.

٥. **انتهاك الخصوصية** ويشمل نشر معلومات ذات طبيعة خاصة عن الأفراد، أو الدخول لحسابات الأفراد الإلكترونية ونشر معلومات عنهم، أو وضع معلومات تخص تاريخ الأفراد ونشرها.

٦. **التصنت** وتشمل الدخول لقواعد المعلومات وسرقة المحادثات عبر الهاتف.

٧. **التجسس** ويشمل اعتراض المعلومات ومحاولة معرفة ما يقوم به الأفراد.

٨. **التشهير** ويشمل استخدام المعلومات الخاصة أو ذات الصلة بالانحراف أو الجريمة ونشرها بشكل القصد منه اغتيال شخصية الأفراد أو الإساءة.

٩. **السرقة العلمية** الكتب والبحوث العلمية الأكاديمية وخاصة ذات الطبيعة التجريبية والتطبيقية.

١٠. **سرقة الاختراعات** وخاصة في المجالات العلمية لاستخدامها أو بيعها.

١١. **الدخول غير القانوني** للشبكات بقصد إساءة الاستخدام أو الحصول على منافع من خلال تخريب المعلومات أو التجسس أو سرقة المعلومات.

١٢. **قرصنة البرمجيات** ويشمل النسخ غير القانوني للبرمجيات واستخدامها أو بيعها مرة أخرى.

١٣. **قرصنة البيانات** والمعلومات ويشمل اعتراض البيانات وخطفها بقصد الاستفادة منها وبخاصة أرقام البطاقة الائتمانية وأرقام الحسابات وكلمات الدخول وكلمات السر.

١٤. **خلاعة الأطفال** وتشمل نشر صور خاصة للأطفال "الجنس السياحي" للأطفال خاصة، وللإناث بشكل عام، ونشر الجنس التخيلي (Cyber Six) على الشبكات.

١٥. **القنابل البريدية** وتشمل إرسال فيروسات لتدمير البيانات من خلال رسالة ملغومة إلكترونية.

١٦. **إفشاء الأسرار**، وتشمل الحصول على معلومات خاصة جداً ونشرها على الشبكة.

١٧. **الإحتيـال المـالي** بالبطاقات وهذا نـاتج عن استخدام غير شرعي لبطاقات التسوق أو الماليـة أو الهاتف ..الخ.
١٨. **سرقة الأرقام والمتاجرة** بها وخاصة أرقام الهواتف السرية واستخدامها في الاتصالات الدولية أو أرقام بطاقات الائتمان.
١٩. **التحرش الجنسي** ويقصد به المضايقة من الذكور للإناث أو العكس من خلال المراسلة أو المهاتفة، أو المحادثة، أو الملامسة.
٢٠. **المطـاردة والملاحقـة والابتـزاز** وتشمل ملاحقة الذكور للإنـاث أو العكس والتتبع بقصد فرض إقامة علاقة ما، وذلك من خلال استخدام البريد الإلكتروني وإرسال الرسائل.
٢١. **الإرهـاب الإلكترونـي**. يشمل جميع المكونات السالفة الذكر في بيئة تقنية متغيرة والتي تؤثر على فرص الإرهاب ومصادرة، هذه التغيرات تؤثر على تكتيكات الإرهاب وأسلحته وأهدافه ومن التكتيكات الإرهابية ما يعرف بالإرهاب الإلكتروني.

المراجع العربية

البحر، عبد الرحمن (١٩٩٩). معوقات التحقيق في جرائم الأنترنت." رسالة ماجستير غير منشورة". الرياض: أكاديمية نايف العربية للعلوم الأمنية.

البداينة، ذياب (٢٠١٣) الرصد والتحليل العلمي لمحتويات الشبكات الاجتماعية في مجال الإرهاب. – ورقة مقدمة في الندوة العلمية توظيف شبكات التواصل الاجتماعي في مكافحة الإرهاب. الرياض ٢٣- ٢٠١٣/٢/٢٧

البداينة، ذياب (٢٠١١) استخدامات الأنترنت في برامج الوقاية من سوء استخدام المخدرات. ورقة مقدمة في الندوة العلمية استخدام الأنترنت في مكافحة المخدرات، جامعة نايف العربية للعلوم الأمنية، الرياض- السعودية، ٩ -٢٠١١/٥/١١

البداينة، ذياب والتوايهه، مريم، والعوران حسن(٢٠١٠). العلاقة بين مستوى ضبط الذات المنخفض والسلوك الطائش لدى طلبة المدارس في الأردن. مجلة العلوم الإنسانية والاجتماعية. جامعة الشارقة.

البداينة، ذياب (ب ٢٠٠٩). **الجريمة الافتراضية.** ورقة مقدمة في الملتقى الدولي **التنظيم القانوني للأنترنت والجريمة الإلكترونية** بجامعة عاشور زيان بالجلفة. الجلفة بالجزائر في الفترة ٢٧-٢٨/ ٤/ ٢٠٠٩

البداينة، ذياب، الطراونة، أخليف، والعثمان، حسين، وأبو حسان ريم (٢٠٠٩). عوامل الخطورة في البيئة الجامعية لدى الشباب الجامعي في الأردن. المجلس الأعلى للشباب: مركز إعداد القيادات الشبابية. البداينة، ذياب (٢٠٠٦). **الأمن وحرب المعلومات.**عمان: دار الشروق.

البداينة، ذياب (٢٠٠٨). **الإرهاب التخيلي**. بحث مقدم إلى الحلقة العلمية الأنترنت والإرهاب. جامعة عين شمس بالتعاون مع جامعة نايف العربية للعلوم الأمنية

البداينة، ذياب؛ الرشيد، صالح؛ المهيزع، ناصر(٢٠٠٥). فحص النظرية العامة للجريمة في المملكة العربية السعودية، **مجلة مؤته للبحوث الدراسات**، المجلد(٢٠). العدد(١)، ص١٤١-١٦٩.

البداينة، ذياب (٢٠٠٣). **الإعلام الأمني في عصر المعلومات**. بحث مقدم إلى الندوة العلمية العمل الإعلامي الأمني : المشكلات والحلول. جامعة مؤتة بالتعاون مع أكاديمية نايف العربية للعلوم الأمنية خلال الفترة من /٦ - ٢٠٠٣/٦/٤

البداينه، ذياب (٢٠٠٢). الأمن وحرب المعلومات.عمان: دار الشروق.
البداينة، ذياب (١٩٩٩). **جرائم الحاسب والإنترنت.** في مركز الدراسات والبحوث ص ص ٩٣-١٢٦ الظواهر الاجرامية المستحدثة وسبل مواجهتها. الرياض: المؤلف.
البداينه، ذياب (١٩٩٩). جرائم الحاسب والانترنت. في مركز الدراسات والبحوث ص ص ٩٣-١٢٦ الظواهر الإجرامية المستحدثة وسبل مواجهتها. الرياض: المؤلف.
البداينه، ذياب (١٩٩٩). **جرائم الحاسب والانترنت.** في مركز الدراسات والبحوث ص ص ٩٣-١٢٦ الظواهر الإجرامية المستحدثة وسبل مواجهتها. الرياض: المؤلف.
البداينة، ذياب (١٩٩٨). هندرة الثقافة الأمنية والتحصين الاجتماعي ضد الجريمة. **الفكر الشرطي**، م٧، ع، ٢، ص ص٩-٢٥

AABS (Assurance and Advisory Business Services), (1998). **2nd Annual Global Information Security Surve**y. Ernst& Young. http://www. Ey.com/security (also a PDF file).
Adeniran, A.I., 2008. The Internet and Emergence of Yahooboys sub-Culture. *International Journal of Cyber Criminology*, 2 (2):368-381;
Al Badayneh, D. (2013). Human Behavior: When and where virtual Society meets physical Society?. *European Journal of Science and Theology, February 2013, Vol.9, No.1, 3-17*
Alshalan, A. (2006). Cyber-crime and Victimization. Unpublished Ph.D Dissertation in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy in Sociology in Department of Sociology, Anthropology, and Social WorkMississippi State University
Anti-Defamation League. (1999). **CyberTerrorism - Terrorism Update**." http://206.3.178.10/ terror/focus/16_focus_a2.html. 1999.
Aransiola, J.O., Asindemade, S.O., 2011. Understanding Cybercrime Perpetrators and the Strategies They Employ. *Cyberpsychology, Behaviour and Social Networking*, 14(12):759.
Arneklev, B. J., Grasmick, H. G., Tittle, C. R. and Bursik, R. J. Jr. (1993). Low Self-Control and Imprudent Behavior**. *Journal of Quantitative Criminology***, Vol. 9, No. 3, pp. 225-247.
Arquilla, John, Ronfeldt, David and Michele Zanini. "Networks, Netwar and Information-Age Terrorism." in Zalmay M. Khalilzhad and John P. White (eds.). The Changing Role of Information in Warfare. Santa Monica, California, Rand, 1999.
BAE Systems Detica and John Grieve Centre for Policing and Security, London Metropolitan University, 2012. *Organised Crime in the Digital Age. Exploring Internet Crimes and Criminal Behaviour.* Boca Raton, FL: CRC Press, Taylor & Francis Group.
Benson, M. L. and Moore, E. (1992). **Are White-Collar and Common Offenders the Same? An Empirical and Theoretical Critique of a Recently Proposed General Theory of Crime**. *Journal of Research in Crime and Delinquency*, Vol. 29, No. 3, pp. 251-272.
Britz, Marjie. 2004. Computer Forensics and Cyber Crime: An Introduction. New Jersey: Pearson Prentice Hall.
Choucri N. and Clark D., (2013). Who controls cyberspace? *Bulletin of the Atomic Scientists* 2013 69: 21—٣

Cohen, Lawrence E., and Marcus Felson. 1979. "Social Change and Crime Trends: A Routine Activity Approach". *American Sociological Review,* 44: 588-608.

Fafinski, S., Dutton, W.H. and Margetts, H., 2010. *Mapping and Measuring Cybercrime.* Oxford Internet Institute Forum Discussion Paper No. 18., June 2010.

Felson, M. (1998). Everyday Life. Thousand Oaks: Prine Forg Press

Felson, M. and Clarke, R.V. (1998) Opportunity Makes the Thief. Police Research Series Paper 98, Policing and Reducing Crime Unit, Research, Development and Statistics Directorate. London: Home Office. Available at: http://www.homeoffice.gov.uk/rds/prgpdfs/fprs98.pdf

Felson, Marcus; and Ronald V. Clarke. 1998. "Opportunity Makes the Theif: Practical Theory for Crime Prevention". Police Research Series. Paper 98. Research, development and Statistics Directorate. London.

Forde, David R. and Leslie W. Kennedy. 1997. "Risky Lifestyles, Routine Activites, and the General Theory Of Crim. "Justice Quarterly 14:265-94.

Gibbs J. and Giever, D. (1994). Self-Control and Its Manifestations Among University Students: An Emperical Test of Gottfredson and Hirschi's General Theory, *Justice Quarterly.*

Gibbs, J., Giever, J. and Kerr, J. S. (1994). Parental Management and Self-Control: An Empirical Test of Gottfredson and Hirschi's General Theory, Paper presented at the Annual Meeting of the American Society of Criminology, Miami, FL.

Gibbs, John J. and Dennis Giever. 1995. "Self-Control and its Manifestations among University Students: An Empirical Test of Gottfredson and Hirschi's Theory." Justice Quarterly 12:231-55.

Giever, D. (1995). An Empirical Assessment of the Core Elements of Gottfredson and Hirschi's General Theory of Crime, Ph. D. Dissertation, Indiana University of Pennsylvania.

Gottfredson, M. R. and Hirschi, T. (1990). A General Theory of Crime, California: Stanford University Press.

Grasmick, H. G., Tittle, C. R., Bursik, R. J. Jr. and Arneklev, B. J. (1993). Testing the Core Empirical Implications of Gottfredson and Hirschi's General Theory of Crime, *Journal of Research in Crime and Delinquency*, Vol. 30, No. 1, pp. 5-29.

Halder, D., & Jaishankar, K. (2011): Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9.

Hale, C. 1996. "Fear of Crime: A Review of The Literature". *International Review of Victimology,* 4: 79-150.

Hassan A. B., Lass D. F. and Makinde J. (2012. Cybercrime in Nigeria: Causes, Effects and the Way out. ARPN Journal of Science and Technology. Vol. 2 No. 7, 626-631

Holt, T.J., Burruss, G.W., Bossler, A.M., 2010. Social Learning and Cyber Deviance: Examining the Importance of a Full Social Learning Model in the Virtual World. *Journal of Crime and Justice*, 33(2):31-61.

http://www.InternetWorldStats.com/

IC3 2004 Internet Fraud - Crime Report. National White Collar Crime Center and the Federal Bureau of Investigation

International Telecommunication Union, 2011. *Understanding Cybercrime: A Guide for Developing Countries*; Explanatory Report to the Council of Europe Cybercrime Convention, ETS No. 185

Jaishankar. K., 2011. Expanding Cyber Criminology with an Avant-Garde Anthology. *In:* Jaishankar, K., (ed.) *Cyber Criminology:*

Kigerl, A., 2012. Routine Activity Theory and the Determinants of High Cybercrime Countries. *Social Science Computer Review,* 30(4):470-486, 470.

Koops, B.J., 2010. The Internet and its Opportunities for Crime. *In:* Herzog-Evans, M., (ed.) *Transnational Criminology Manual.* Nijmegen, Netherlands: WLP, pp.735-754.

Laura Ani (2011): "Cyber Crime and National Security: The Role of the Penal and Procedural Law

Leukfeldt, R. and Veenstra S., & Stol W.,(2013). High Volume Cyber Crime and the Organization of the Police: The results of two empirical studies in the Netherlands. International Journal of Cyber Criminology (IJCC) ISSN: 0974 – 2891 January – June 2013, Vol 7 (1): 1–17

Meke Eze Stanley, N. (2012): An article "Urbanization and Cyber Crime in Nigeria: Causes and Consequences".

Messner, Steven; and Blau, Judith. 1987. "Routine Activities and Rates of Crime: A Macro-Level Analysis". *Social forces,* 65: 1035-1052.

Miethe, Terance; Stafford, Mark C.; and Long, J. Scott. 1987. " Social Differentiation in Criminal Victimization: A Test of Routine Activities/ Life style Theories". *American Sociological Review,* 52: 184-194.

PCCIP (President s Commission on Critical Infrastructure Protection),(1997). Critical Foundations: Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection, October 1997, p.15; http://WWW.pccip.gov.Also a PDF file.

Pocar, F., 2004. New challenges for international rules against cyber-crime. *European Journal on Criminal Policy and Research,* 10(1):27-37; Wall, D.S., 2007. *Cybercrime: The Transformation of Crime in the Information Age.* Cambridge: Polity Press.

Sinrod E. J., and Reilly W. P., (2013). Cyber-crimes: A Practical Approach to the Application of Federal Computer Crime Laws. Computer and High technology law Journal. Vol. 16., 1-50, MSW file.

Skinner, W.F., Fream, A.M., 1997. A Social Learning Theory Analysis of Computer Crime among College Students. *Journal of Research in Crime and Delinquency*, 34(4):495-518.

Torosyan, Angela (2003). Cyber Crime Programs By Satae and Local Law Enforcement: A preliminary Analysis of A Narional Survey. Unpublished Thesis. California State University.

UNODC United Nations Office on Drugs and Crime (2013).Comprehensive Study on Cybercrime. United nations.

Warner, J., 2011. Understanding Cybercrime: A View from Below. *International Journal of Cyber Criminology*, 5(1):736-749.

Yar, M., 2005. The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology,* 2(4):407-427.

Zager, M. A. (1993). Explicating and Testing A General Theory of Crime, Ph. Dissertation, The University of Arizona.